REMARKS

Claims 2-4, 10-12, 16, 17, 20-22, 26, 27, 30-32, 36 and 37 are pending in the present application. Claims 2-4 were canceled; claims 10, 16, 20, 26, 30, and 36 were amended; and no claims were added. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness, claims 2-4, 10-12, 16-17, 20-22, 26, 27, 30-32, 36 and 37

The Office Action has rejected claims 2-4, 10-12, 16-17, 20-22, 26, 27, 30-32, 36 and 37 under 35 U.S.C. § 103(a) as being unpatentable over Arnold et al. (U.S. Patent No. 5,440,723) in view of Touboul (U.S. Patent No. 6,658,465 B1). This rejection is respectfully traversed.

Regarding claims 10, 20, and 30, the Office Action states:

> Claims 10,20,30: Arnold disclose receiving at a bait server a request to perform a function on the bait server and identifying an offending system which the request originated in (col.25,lines 58-68 and col.26, lines 1-2). Arnold discloses alerting a local server that a virus is in progress and of the identity of the offending system in (col.2,lines 66-68 and col.24,lines 31-42).
> Arnold does not specifically disclose disconnecting the offending system from the network.
> Touboul's patent discloses disconnecting the offending system from the network in (col.5,lines 60-64). It would have been obvious to person of ordinary skill in the art at the time invention was made to disconnect offending system from the network as taught in Touboul with security system of Arnold in order to completely isolate offending system from attacks,spreading virus within the network.

Office Action dated November 15, 2005, page 2

The Office Action bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

Amended independent claim 10, which is representative of amended independent claims 20 and 30 with regards to similarly recited subject matter, recites:

10. A method for detecting the presence of a computer virus, the method comprising;

receiving, at a bait server, a request for access to the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress;

identifying an offending system from which the request originated;

alerting a local server that the virus attack is in progress and of the identity of the offending system; and

disconnecting the offending system from the network.

In comparing Arnold to the claimed invention, the claim limitations of the presently claimed invention may not be ignored in an obviousness determination. More specifically, claim 1 of the present invention recites the feature of "receiving, at a bait server, a request for access to the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress." Such a feature is not taught or suggested by Arnold. The Office Action points to column 1, lines 66 through 67 of Arnold, reproduced below for the Examiner's convenience, as teaching "wherein the bait server's address is not published to a network":

> However, conventional virus scanners are typically unable to detect the presence of computer viruses which they have not been programmed to detect explicitly.

(Arnold, col. 1, line 66 – col. 2, line 1)

The first passage of Arnold cited above, column 1, line 66 through column 2, line 1, does not teach the feature of "wherein the bait server's address is not published to a network." Instead, the passage simply explains that many virus scanners are unable to detect any virus that they have not been specifically programmed to detect. The passage has nothing to do with a bait server and not publishing the bait server's address to the network.

Furthermore, Arnold teaches a "decoy" server, wherein the address of the dummy server is known to all members of the network, as explained in column 25, lines 52 through 65, reproduced below for the Examiner's convenience:

> If the computer on which the immune system is installed is part of a network (e.g. a LAN), the decoy programs may be deployed on another machine, preferably the dedicated processor P_D of FIG. 1*b*. In this case, any modified

executables are sent over the network from the infected computer to the decoy server P_D, which performs the functions described above. It is thus assumed that the decoy server P_D is reachable from and by all processors connected to the network. The decoy server P_D sends the results back to the infected computer over the network. By running the decoy programs on the physically distinct decoy server P_D the risk of creating further copies of the virus on the infected machine is reduced.

(Arnold, col. 25, lines 52-65, emphasis added)

The above cited passage of Arnold says that "any modified executables are sent over the network from the infected computer to the decoy server." In order for the infected machine to send the modified executables to the decoy server, the infected machine must know the address of the decoy server. Additionally, Arnold explicitly teaches that "the decoy server is reachable from and by all the processors connected to the network." In order for all the processors to be able to reach the decoy server, the processors must know the address of the server. Therefore, Arnold teaches that the address of the decoy server is published to all the clients in the network. Thus, Arnold cannot teach the feature of "wherein the bait server's address is not published to a network," as Arnold actually teaches away from this feature.

The Office Action points to column 25, line 58 through column 26, line 2, reproduced below for the Examiner's convenience, as teaching receiving a request for access to a bait server at the bait server, wherein receipt of the request indicates that a virus attack is in progress:

The decoy server could return control to the infected machine at a number of points (after Blocks K, L, M, or N), but preferably the decoy processor performs Blocks J, K, L, M, and N so as to reduce the risk of further contamination of the infected machine.

(Arnold, col. 25, line 66 – col. 26, line 2)

The above cited passage of Arnold dos not teach receiving a request for access to a bait server at the bait server, wherein receipt of the request indicates that a virus attack is in progress. Instead, the above cited passage of Arnold teaches that in various implementations, the decoy server could stop and return control of the process to the infected machine at any number of points; but, in a preferred embodiment the decoy server performs blocks J, K, L, M, and N of Figure 3 before returning control to the infected machine. Blocks J, K, L, M, and N of Figure 3 are steps for

identifying the virus and extracting its signature if the virus was previously unknown. However, the decoy programs are not deployed onto the decoy server and blocks J, K, L, M, and N are not executed until after a virus has already been detected (see Arnold, col. 25, lines 52-65; Figure 3). Therefore, Arnold does not teach the feature of "wherein receipt of the request indicates that a virus attack is in progress" because, as taught by Arnold, a virus has already been detected before the client ever contacts the decoy server and the request is a request to try and determine the identity of the already detected virus. In contradistinction, as recited in claim 1 of the present invention, it is the receipt of a request from the network by the bait server for access to the bait that indicates that a virus is present. Since the network does not know the address of the bait server, the network cannot send a request to the bait server. Therefore, the fact that the bait server received a request for access indicates that some malicious entity, such as a virus or worm, is now trying to gain access.

Touboul does not cure the deficiencies of Arnold. Touboul does not teach the feature missing from Arnold, "receiving, at a bait server, a request for access to the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress," nor does the Office Action point to any portion of Touboul that teaches this feature. Touboul teaches a system for monitoring and controlling programs executed on a workstation (see Touboul, Abstract).

Thus, even if one were to combine the teachings of Arnold and Touboul, the resulting combination would not teach receiving, at a bait server, a request for access to the bait server, wherein the bait server's address is not published to a network and wherein receipt of the request indicates that a virus attack is in progress, as recited in claim 10 of the present invention. Instead, the combination of Arnold in view of Touboul would teach a system that detects a computer virus, deploys decoy programs and a copy of the virus from an infected machine to a decoy server, wherein the decoy server attempts to identify the unknown virus, whereupon the decoy server would notify both the infected machine and the network administrator of the results. Therefore, the combination of Arnold in view of Touboul would not reach the presently claimed invention.

Therefore, for all the reasons set forth above, Applicants submit that amended independent claims 10, 20, and 30 are patentable over the cited references because the combination of Arnold in view of Touboul does not teach or suggest the presently claimed

invention. As claims 11, 12, 17, 21, 22, 27, 31, 32, and 37 are dependent claims depending from amended independent claims 10, 20, and 30, respectively, the same distinctions between the combination of Arnold in view of Touboul and the claimed invention in claims 10, 20, and 30 apply for these claims. Therefore, Applicants respectfully submit that claims 11, 12, 17, 21, 22, 27, 31, 32, and 37 are patentable over the cited combination of Arnold in view of Touboul at least by the virtue of their depending from an allowable claim. Additionally, claims 12, 22, and 32 recite features not taught by the cited references.

Claims 12, 22, and 32 recite the features of "receiving a reconnect request from the offending system;" "verifying that the offending system is disinfected and available to reconnect to the network;" and "reconnecting the offending system to the network." The Office Action does not point to any passage of either Arnold or Touboul as teaching or suggesting these features, nor does any passage of either Arnold or Touboul teach these features. Instead, in rejecting these claims the Office Action takes Official notice that "notifying the offending system that it is infected with a virus prior to disconnecting the system is well known in the art." However, this Official notice does not address any of the features recited in claims 12, 22, and 32.

Claims 17, 27, and 37 recite the features of "instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication." The Office Action does not point to any passage of either Arnold or Touboul as teaching or suggesting this feature, nor does any passage of either Arnold or Touboul teach this feature. Instead, in rejecting these claims the Office Action takes Official notice that "notifying the offending system that it is infected with a virus prior to disconnecting the system is well known in the art." However, this Official notice does not address any of the features recited in claims 17, 27, and 37. Furthermore, Arnold teaches away from the claimed features. Rather than instructing all other devices in the network to ignore requests from the infected machine, Arnold teaches continued communication with the infected machine. In column 25, lines 52 through 65, quoted above, Arnold teaches that the decoy server receives requests from a machine known to be infected and performs the requested action and then communicates back with the infected machine. Additionally, in column 19, line 46 through column 20, line 11, Arnold explains how infected machines communicate with other machines in the network to tell them of the infection. As such, the network is listening to the infected

machine. Additionally, nowhere in this passage or in any other passage does Arnold describe telling the other machines in the network to ignore the infected machine as part of the message or in any other message.

Regarding claims 16, 26, and 36, the Office Action states:

> Claims 16,26,36:Arnold disclose monitoring the network for the presence of a computer virus in (col.4,lines 60-68;col.5,line 1). Arnold discloses not publishing the bait server's address to the network in (col.1, lines 66-7). Arnold discloses alerting a local server that a virus is in progress and of the identity of the offending system in (col.2,lines 66-68 and col.24,lines 31-42). Arnold does not specifically disclose disconnecting the offending system in (col.2,lines 66-68 and col.24,lines 31-42). Arnold does not specifically disclose disconnecting the offending system from the network. Touboul's patent discloses disconnecting the offending system from the network in (col.5,lines 60-64). It would have been obvious to person of ordinary skill in the art at the time invention was made to disconnect offending system from the network as taught in Touboul with security system of Arnold in order to completely isolate offending system from attacks,spreading virus within the network. Further, directing all devices to ignore a communication requests from offending system would have been obvious in order to stop any virus from entering the network.

Office Action dated November 15, 2005, pages 2-3

Amended independent claim 16, which is representative of amended independent claims 26 and 36 with regards to similarly recited subject, recites:

> 16. A method in a bait server for detecting the presence of a computer virus, the method comprising:
>
> not publishing the bait server's address to a network;
>
> receiving a request for access from the network, wherein receipt of the request indicates that a virus is present;
>
> determining the identity of an offending system within the network from which the virus entered the network;
>
> notifying a local server of the presence of the virus and the identity of the offending system;
>
> instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication;
>
> directing the local server to disconnect the offending system from the network; and

responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, reconnecting the offending system to the network.

Claim 16 recites the features of "not publishing the bait server's address to a network;" "receiving a request for access from the network, wherein receipt of the request indicates that a virus is present;" and "responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, reconnecting the offending system to the network." As discussed above regarding claim 10, neither Arnold, Touboul nor the combination of Arnold in view of Touboul teaches the features of "not publishing the bait server's address to a network;" "receiving a request for access from the network, wherein receipt of the request indicates that a virus is present." Additionally, as discussed above regarding claim 12, neither Arnold, Touboul nor the combination of Arnold in view of Touboul teaches the feature of "responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system to the local server, reconnecting the offending system to the network."

Therefore, for all the reasons set forth above, Applicants submit that amended independent claims 16, 26, and 36 are patentable over the cited references because the combination of Arnold in view of Touboul does not teach or suggest the presently claimed invention.

Therefore, the rejection of claims 2-4, 10-12, 16-17, 20-22, 26, 27, 30-32, 36 and 37 under 35 U.S.C. § 103 has been overcome.

II. Conclusion

For all the above reasons, it is respectfully urged that claims 10-12, 16, 17, 20-22, 26, 27, 30-32, 36, and 37 are allowable in their present form, and that this application is now in condition for allowance. It is, accordingly, respectfully requested that the Examiner so find and issue a Notice of Allowance in due course.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: Feb. 14, 2006

Respectfully submitted,

Gerald H. Glanzman
Reg. No. 25,035
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

GHG/bj